



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/830,392	06/18/2001	Yoshihito Ishibashi	450108-02659	6916
20999	7590	02/09/2005	EXAMINER	
FROMMER LAWRENCE & HAUG 745 FIFTH AVENUE- 10TH FL. NEW YORK, NY 10151			DADA, BEEMNET W	
		ART UNIT	PAPER NUMBER	
		2135		
DATE MAILED: 02/09/2005				

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	09/830,392	ISHIBASHI ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Beemnet W Dada	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 18 August 2004.

2a) This action is **FINAL**.                                    2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1-128 is/are pending in the application.

4a) Of the above claim(s) 1-68,118-147 and 171-218 is/are withdrawn from consideration.

5) Claim(s) \_\_\_\_\_ is/are allowed.

6) Claim(s) 69-117, 148-170 is/are rejected.

7) Claim(s) \_\_\_\_\_ is/are objected to.

8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All    b) Some \* c) None of:

1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) Notice of References Cited (PTO-892)

2) Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 6/18/01.

4) Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.

5) Notice of Informal Patent Application (PTO-152)

6) Other: \_\_\_\_\_.

## **DETAILED ACTION**

1. Applicant's election without traverse of Group II claims 69-117 and 148-170 in the reply filed on August 18, 2004 is acknowledged.
2. Claims 69-117 and 148-170 are examined.

### ***Claim Rejections - 35 USC § 112***

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 69, 70, 75-86, 88-94 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 69, 70, 75-86, 88-94 recites the limitation "said data". There is insufficient antecedent basis for this limitation in the claim. The term "said data" is preceded by terms including "predetermined data", "key data" and "send data", and it is not clear which one of the above "said data" is referring to. Appropriate correction is required.

### ***Claim Rejections - 35 USC § 102***

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 69-71, 75, 79, 83, 87 and 91 are rejected under 35 U.S.C. 102(e) as being anticipated by Momiki et al. US Patent 6,097,816 (hereinafter Momiki).

7. As per claims 69-71, 75, 79, 83, 87 and 91, Momiki teaches an information distribution system for distributing predetermined data from an information sending device to an information receiving device, characterized in that

said information sending device comprises: sending means for sending send data including data encrypted with key data for distribution given in advance [column 8, lines 18-34], and

said information receiving device comprises: receiving means for receiving said send data and receiving end controlling means for decrypting data using said key data given in advance [column 8, lines 35-39].

### ***Claim Rejections - 35 USC § 103***

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claim 72-74, 76-78, 80, 81, 82, 84-86, 88-90 and 92-94 are rejected under 35 U.S.C. 103(a) as being unpatentable over Momiki US Patent 6,097,816 in view of Horne US Patent 4,887,296.

10. As per claims 72-74, 76-78, 80, 81, 82, 84-86, 88-90 and 92-94, Momiki teaches an information distribution system as applied above. Momiki further teaches transmitting encrypted data and decrypting the encrypted data with a key data given in advance [column 8, lines 18-39]. Momiki is silent on the key data being individual key that is specific to a device and said key data that is periodically updated. However, the system of generating encryption/decryption keys that are specific to a device and are periodically updated is old and well known in the art. For example, within the same field of endeavor Horne teaches a cryptographic system for data transmission, including a method for providing individual keys that are specific to a device [column 3, lines 63 – column 4, lines 14], and further, including periodically changing keys at a time interval [column 4, lines 41-44], which has the advantage of transmitting data only to a specific authorized device securely. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Horne within the system of Momiki in order to further enhance the security of the system by changing keys periodically and providing individual keys as taught by Horne.

11. Claim 95-117 and 148-170 are rejected under 35 U.S.C. 103(a) as being unpatentable over Richards US Patent 6,690,795 B1 in view of Horne US Patent 4,887,296.

12. As per claims 95-117, Richards teaches an information distribution system for distributing predetermined content data from an information sending device to an information receiving device [see abstract] characterized in that:

    said information sending device comprises: sending end controlling means for encrypting content data with a key SK [column 8, lines 37-43], and encrypting the key SK with a second key PK [column 9, lines 14-16]; and encrypting the second key PK with a predetermined third key (Customer Code) [column 9, lines 16-17], and transmitting the encrypted content, encrypted content key and encrypted second key PK [column 9, lines 19-25 and column 8, lines 31-42].

    said information receiving device comprises: receiving means for receiving the encrypted content encrypted with the content key (SK), the control key encrypted with the second key (PK) and the encrypted second key [column 9, lines 19-25 and column 8, lines 31-42]; and receiving end controlling means for decrypting the second key (PK) with the third key (Customer Code) that is given in advance, and decrypting the content key (SK) with the decrypted second key (PK), and decrypting the content with the content key [column 9, lines 24-44]. Furthermore, Richards teaches periodically changing content key (SK) and second key (PK) [column 8, lines 32-35]. Richards is silent on the second key being individual key that is specific to a device. However, within the same field of endeavor Horne teaches a cryptographic system for data transmission, including a method for providing individual keys that are specific to a device, wherein the individual keys encrypt content key used for encrypting content [column 3, lines 63 – column 4, lines 14], and further, including periodically changing keys at a time interval [column 4, lines 41-44], which has the advantage of transmitting data only to a specific authorized device securely. Therefore it would have been obvious to one having ordinary skill in the art at the time

the invention was made to employ the teachings of Horne within the system of Richards in order to further enhance the security of the system by providing individual keys as taught by Horne.

13. As per claims 148-170, Richards teaches an information distribution system for distributing predetermined content data from an information sending device to an information receiving device [see abstract] characterized in that:

    said information sending device comprises: sending end controlling means for encrypting content data with a key SK [column 8, lines 37-43], and encrypting the key SK with a second key PK [column 9, lines 14-16]; and encrypting the second key PK with a predetermined third key (Customer Code) [column 9, lines 16-17], and transmitting the encrypted content, encrypted content key and encrypted second key PK [column 9, lines 19-25 and column 8, lines 31-42].

    said information receiving device comprises: receiving means for receiving the encrypted content encrypted with the content key (SK), the control key encrypted with the second key (PK) and the encrypted second key [column 9, lines 19-25 and column 8, lines 31-42]; and receiving end controlling means for decrypting the second key (PK) with the third key (Customer Code) that is given in advance, and decrypting the content key (SK) with the decrypted second key (PK), and decrypting the content with the content key [column 9, lines 24-44]. Furthermore, Richards teaches periodically changing content key (SK) and second key (PK) [column 8, lines 32-35], including changing keys SK and PK after the content has been decrypted [column 9, lines 40-51]. Richards is silent on the second key being individual key that is specific to a device. However, within the same field of endeavor Horne teaches a cryptographic system for data transmission, including a method for providing individual keys that are specific to a device, wherein the individual keys encrypt content key used for encrypting content [column 3, lines 63

– column 4, lines 14], and further, including periodically changing keys at a time interval [column 4, lines 41-44], which has the advantage of transmitting data only to a specific authorized device securely. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to employ the teachings of Horne within the system of Richards in order to further enhance the security of the system by providing individual keys as taught by Horne.

### ***Conclusion***

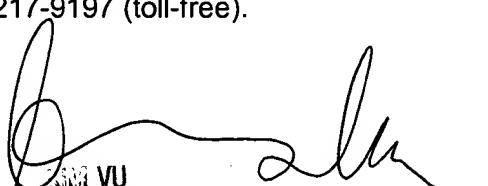
14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada



KIM Y VU  
PRESIDING PATENT EXAMINER  
TECHNOLOGY CENTER 21